

**Escuela Colombiana De Ingeniería
Julio Garavito**

Seguridad y privacidad TI

Daniel Esteban Vela Lopez

Andres Felipe Montes

Laura Valentina Rodriguez Ortegón

Laboratorio No.2

2024-2

Nivel 0 = ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

para el nivel 0 ya nos encontrábamos en el directorio de inicio y se utilizó el comando ls para listar los directorios que se encuentran dentro de la carpeta, luego usamos el pwd para mostrar el directorio de trabajo actual y por último cat readme, el cual nos muestra el contenido de los archivos

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ pwd
/home/bandit0
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
```

```
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\andres.montes> ssh bandit1@bandit.labs.overthewire.org -p 2220
```



This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

Nivel 1= 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Para el nivel 1 vamos a ingresar con la contraseña del primer nivel y aplicamos los comandos anteriores, según el orden para mostrar los archivos dentro del directorio, buscamos nuestro archivo "-" pero con la ruta completa, entonces va ir desglosando desde el

/home

/bandit1

/-

```
bandit1@bandit:~$ pwd
/home/bandit1
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat /home/bandit1/-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

```
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\andres.montes> ssh bandit2@bandit.labs.overthewire.org -p 2220
```

Nivel 2 = MNk8KNH3Usiio41PRUEoDFPqfxLPIsmx

Para este nivel 2, vamos a tener en cuenta la dirección de la ruta para bandit2 y como es un nombre con espacios debería ir entre comillas para que no afecten los espacios y no agregue otros símbolos especiales a la hora de la búsqueda, si no que más bien va a tomar el nombre textualmente.

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ pwd
/home/bandit2
bandit2@bandit:~$ cat /home/bandit2/"spaces in this filename"
MNk8KNH3Usiio41PRUEoDFPqfxLP1Smx
bandit2@bandit:~$
```

```
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\andres.montes> ssh bandit3@bandit.labs.overthewire.org -p 2220
```

[_ _ _ _ _] [_ _ _ _ _]
 [_ \ / _ \ / _ \ / _ \ / _]
 [_ \ / _ \ / _ \ / _ \ / _]
 [_ _ _ _ _] [_ _ _ _ _]

This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

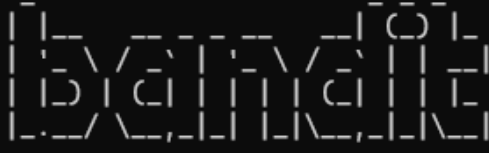
Nivel 3 = 2WmrDFRmJlq3IPxneAaMGhap0pFhF3NJ

Para el nivel 3 seguimos en el directorio de `inhere` y con el comando `ls -a` vamos a listar los directorios que están ocultos, en este caso nos va salir el archivo oculto `..`

...Hiding-From-You, lo leemos y nos dara la contraseña correspondiente

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -la
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$
```

```
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\andres.montes> ssh bandit4@bandit.labs.overthewire.org -p 2220
```



This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

Nivel 4= 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Volvemos a realizar el pasó anterior para listar los directorios ocultos desde el /bandit3, pero acá empezamos a revisar los archivos para localizar la contraseña y nos damos cuenta que estan corruptos, entonces buscamos el que nos muestre la contraseña correcta, hasta encontrarla en el archivo -file07, mostraremos la información con el comando de cat ./-file07, lo buscamos así para que no tenga inconvenientes por el símbolo especial

```
Try 'cat --help' for more information.
bandit4@bandit:~/inhere$ ls -la
.  .. -file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ cat .
./ ./
bandit4@bandit:~/inhere$ cat .
./ ./
bandit4@bandit:~/inhere$ cat .
./ ./
bandit4@bandit:~/inhere$ cat ./
cat: ./: Is a directory
bandit4@bandit:~/inhere$ cat ./-file0
cat: ./-file0: No such file or directory
bandit4@bandit:~/inhere$ cat file00
cat: file00: No such file or directory
bandit4@bandit:~/inhere$ cat ./-file00
??,??s???Yq??f?L???j?s?0???x?4Fbandit4@bandit:~/inhere$ cat ./-file01
N?.?bandit4@bandit:~/inhere$ cat ./-file02
??9?????F??p?????t?k???%??bandit4@bandit:~/inhere$ cat ./-file03
????n?Qy?y_ ?{+R?bZ?k?F?*      bandit4@bandit:~/inhere$ cat ./-file04

l?????]?a?-@gQ?÷?wz?P?Ty?bandit4@bandit:~/inhere$ cat ./-file05
?p?T9?F?3? ????
T? F?ç?bandit4@bandit:~/inhere$ cat ./-file06
?Q?L?M???p4?-?8??=?!!#g???bandit4@bandit:~/inhere$ cat ./-file04
l?????]?a?-@gQ?÷?wz?P?Ty?bandit4@bandit:~/inhere$ cat ./-file06
?Q?L?M???p4?-?8??=?!!#g???bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$
```

```
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\andres.montes> ssh bandit5@bandit.labs.overthewire.org -p 2220
```

```

  _ _ _ _ _
 | | | | |
 | | | | |
 | | | | |
 | | | | |

```

This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

```
bandit5@bandit.labs.overthewire.org's password:
```

Nivel 5 = HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Como las búsquedas se hacen con muchos más archivos de los que teníamos antes, entonces ahora vamos a implementar la búsqueda con comando find rutaDelArchivo -type f -size 1033c, donde la idea es buscar los parámetros que se dan desde la búsqueda hasta el tamaño de archivo, en este caso nos vamos a la ruta de

```
/home
```

```
/bandit5
```

y desde ahí va buscar el archivo correspondiente, obteniendo el archivo de 1033 bytes correspondiente

```
bandit5@bandit:~/inhere/maybehere00$ find /home/bandit5/inhere -type f -size 1033b
bandit5@bandit:~/inhere/maybehere00$ pwd
/home/bandit5/inhere/maybehere00
bandit5@bandit:~/inhere/maybehere00$ cd ..
bandit5@bandit:~/inhere$ find /home/bandit5/inhere -type f -size 1033c
/home/bandit5/inhere/maybehere07/.file2
bandit5@bandit:~/inhere$ pwd
/home/bandit5/inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat .file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

Nivel = 6 morbNTDkSW6jIlUc0ymOdMaLnOIFVAaj

Acá vamos a filtrar por el usuario, grupo y tamaño del archivo. Donde pedimos que busque cada información en el directorio deseado y al final del comando el redirecciona la salida estándar de errores (stderr), al dispositivo nulo (/dev/null)

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOIFVAaj
bandit6@bandit:~$
```

Nivel 7 = dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Para el nivel 7, vamos a usar grep en este caso la palabra millionth será nuestro filtro en el archivo .txt, donde va buscar esa palabra en específico y nos mostrará la contraseña para el siguiente nivel.

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ pwd
/home/bandit7
bandit7@bandit:~$ grep "millionth" data.txt
millionth      dfwvzFQi4mU0wfNBFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

Nivel 8 = 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Para este punto vamos a buscar el archivo data.txt y vamos agrupar y ordenar las líneas con el comando sort, asegurando que se muestran el número de todas las líneas duplicadas con -cc, ya que elimina las líneas duplicadas y a la vez las va contando sobre el archivo data.txt.

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -c
10 0KCctkqCfY7BIOwqoLXsHDaboXVTKZ49
10 1SKCEfQ151hW0x9JkeIAmOQdXiC813h1
10 3hHLoFjM7m3sdyiKJF5QsMqvEIfFh5b1
10 3hW8tLnDV8acjhTQi44CKXEzHsJb3sqz
10 3nUXvAjKo7yu6fYykYu7nGGKDMuNMWZf
10 42qjuz5hdLlItNwdJYsDRpkbbvoEYiWK
1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
10 5n2sVU0okwgDy29Pfo6C7twiKcOkUwQV
```

```
bandit8@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\andres.montes> ssh bandit9@bandit.labs.overthewire.org -p 2220
```

```

  _ _ _ _ _
 | | | | |
 | | | | |
 | | | | |
 | | | | |
  _ _ _ _ _

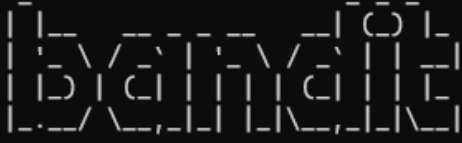
```

This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

Nivel 9 = FGUW5iILVJrxX9kMYMmlN4MgbpfMiqey

Para este nivel solo es necesario leer la información del archivo data.txt con el comando cat y a partir de lo que se muestra es fácil descifrar la contraseña porque la otra información está corrupta, así que no hay que evaluar muchos puntos para resolver cual es la contraseña.


```
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\andres.montes> ssh bandit11@bandit.labs.overthewire.org -p 2220
```



This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>


Nivel 11 = 7x16WNeHli5YklhWsfFIqoognUTyj9Q4

En este nivel leemos nuestro archivo y nos podemos dar cuenta que no hay ningún patrón ordenado, así que lo que se debe hacer es empezar a seguir la forma en que está almacenada la información, como no lo dice en el enunciado, “todas las letras minúsculas (az) y mayúsculas (AZ) se han rotado 13 posiciones”, entonces en este comando que se ha utilizado es para realizar una transformación de texto en un archivo, aplicando una técnica conocida como cifrado ROT13 . Este tipo de cifrado es un caso especial de un cifrado, donde cada letra del alfabeto es sustituida por la letra que se encuentra 13 posiciones después en el alfabeto.

Lo que está haciendo es transformar caracteres en la entrada estándar, la cual vendría siendo desde la a hasta la z, desde la entrada que se da que es de rotación cada 13 posiciones, haciendo que el contenido se organice como se esperaría del archivo data.txt

```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
bandit11@bandit:~$ tr 'A-Za-z' 'N-ZA-Mn-za-m' < data.txt
The password is 7x16WNeHli5YklhWsfFIqoognUTyj9Q4
bandit11@bandit:~$
```

```
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\andres.montes> ssh bandit12@bandit.labs.overthewire.org -p 2220
```



This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

Nivel 12 = FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn

Para el nivel 12 se sugiere a los participantes crear un directorio temporal para poder trabajar más libremente, entonces eso fue lo primero que se hizo con el comando mktemp.

Después de eso se vuelve a usar el comando file para verificar si data seguía comprimido y de qué forma se había hecho, el método de compresión esta vez fue gzip por que se renombro el archivo con un .gz para descomprimirlo utilizando el comando gunzip dando como resultado otra vez data

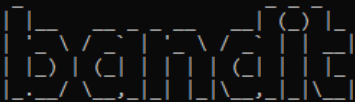
```

bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ ls
data1.txt data2.txt
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data1.txt
data1.txt: ASCII text
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ cat data1.txt | xxd -r > data
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ ls
data data1.txt data2.txt
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data
data: gzip compressed data, was "data2.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, original size modulo 2^32 577
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ mv data.data.gz
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ gunzip data.gz
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file
Usage: file [-bcdEhikllNnprrSvz0] [--extension] [--mime-encoding]
        [--mime-type] [-e <testname>] [-F <separator>] [-f <filename>]
        [-m <magicfiles>] [-P <parameter=value>] [--exclude-quiet]
        [<file> ...
    file -C [L= <magicfiles>]
    file --help
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ ls
data data1.txt data2.txt
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ cat data
ggh1hpqA9Bjw1B1[('O',8A3">`& J1Hefid&RQmQt]jFWk6jYPJ0m0u9d0BbbJ+M*O1l&0&,IG:Ier'dGHH_X0m=VAQ0000(G"bt:U@t">2&W"BUW0000x.009AB/QzHEIK@'DPK:'S
(B0< cJ;cjy0MB0*)"SHn
w3A>*Y(00(2HK100-B7-7h000 m3E510u1/00PN_H
00D0bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data
data: bzip2 compressed data, block size = 900K
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ mv data.data.bz2
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ bunzip2 data.bz2
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data
data: gzip compressed data, was "data4.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ cat data
cEVBU8A#@#I)8mm00((0yyYw0e.n1'f')-sbu0m00GH--BV9B)RMZpV0X\
hb06)F&2tk0j0)3]>jYBA02E,Bd7w:G+XWYT(C3BaEtjEvoilM**Vu0Re5B k2BHor(km7x:+3ENd0EDVR\YLm-8kB@EPbandit12@bandit:/tmp/tmp.F8ZV9qtKp$ mv data.data.gz
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ gunzip data.gz
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ cat data
data5.bin000064400000000000000000240014645764722011261 0ustar rootrootdata6.bin0000644000000000000000000033514641 ih0EFNM0i:ibdaAH8 700[B sbu0**h07[X@BS0G@8BA1B3']!DE]k.,1+N([Z00r0UF0
E.pl_"bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ tar -xvf data
data5.bin
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ cat data5.bin
I ih0EFNM0i:ibdaAH8 700[B sbu0**h07[X@BS0G@8BA1B3']!DE]k.,1+N([Z00r0UF0*>BP00i< E.pl_"bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ tar -xvf data5.bin
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ ls
data data1.txt data2.txt data5.bin data6.bin
data data1.txt data2.txt data5.bin data6.bin
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ cat data6.bin
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ cat data6.bin
I ih0EFNM0i:ibdaAH8 700[B sbu0**h07[X@BS0G@8BA1B3']!DE]k.,1+N([Z00r0UF0*>BP00i< E.pl_"bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900K
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ bunzip2 data6.bz2
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ cat data6
L6KB.biq)w02AIbandit12@bandit:/tmp/tmp.F8ZV9qtKp$ 11267 0ustar rootrootdata9.bin000HU(H,.../Q,Vp7H)w+NGHNJ0023
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ tar -xvf data6
data8.bin
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Wed Jul 17 15:57:06 2024, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ mv data8.bin data8.gz
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ gunzip data8.gz
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ file data8
data8: ASCII text
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$ cat data8
The password is F05dwFsc0cba1IH0h8J2eUks2vdT0dAn
bandit12@bandit:/tmp/tmp.F8ZV9qtKp$

```

Es importante establecer conexión de forma segura a través de SSH a un servidor remoto, para este caso el mismo localhost, el cual va utilizar una clave privada en vez de ser una contraseña. con el fin de utilizar un nivel adicional de seguridad, luego de esto si podemos ubicarnos en el directorio de `/etc/bandit_pass/bandit14`, acá ingresaremos a este directorio, leeremos la info de `bandit14`; la contraseña para el siguiente nivel y la encontraremos

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
```



```

      This is an OverTheWire game server.
  More information on http://www.overthewire.org/wargames

!!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!!! Connecting from localhost is blocked to conserve resources.
!!! Please log out and log in again.
```

```
bandit14@bandit:~$ pwd
/home/bandit14
bandit14@bandit:~$ ls
bandit14@bandit:~$ cd /etc/bandit_pass
bandit14@bandit:/etc/bandit_pass$ ls
bandit0  bandit12  bandit16  bandit2  bandit23  bandit27  bandit30  bandit4  bandit8
bandit1  bandit13  bandit17  bandit20  bandit24  bandit28  bandit31  bandit5  bandit9
bandit10 bandit14  bandit18  bandit21  bandit25  bandit29  bandit32  bandit6
bandit11 bandit15  bandit19  bandit22  bandit26  bandit3  bandit33  bandit7
bandit14@bandit:/etc/bandit_pass$ cat bandit14
MU4VWeTyJk8R0of1qqmcBPALh7lDCPvS
bandit14@bandit:/etc/bandit_pass$
```

Enjoy your stay!

```
bandit14@bandit:~$
```

Nivel 14 = 8xCjnmgoKbGLhHFAZIGE5Tmu4M2tKJQo

En este nivel usamos el comando el cual se utiliza para enviar un mensaje, que en este caso es la contraseña, que se usó para entrar al nivel, a un servicio o aplicación que está escuchando en un puerto específico; donde es el 30000 en la máquina local (localhost) utilizando nc (Netcat), este puede leer y escribir datos a través de conexiones de red utilizando TCP o UDP, en este caso va a leer la contraseña.

```
bandit14@bandit:~$ ls
bandit14@bandit:~$ echo "MU4VWeTyJk8R0of1qqmcBPALh7lDCPvS" | nc localhost 30000
Correct!
8xCjnmgoKbGLhHFAZIGE5Tmu4M2tKJQo
bandit14@bandit:~$
```

Nivel 15 = 8xCjnmgoKbGLhHFAZIGE5Tmu4M2tKJQo

Al ejecutar openssl s_client -connect localhost:30001, el comando establece una conexión SSL/TLS con el servicio que escucha en el puerto 30001 de la máquina local, permitiendo verificar que el servicio esté operando correctamente y que la configuración SSL/TLS sea válida. Además, proporciona detalles sobre la conexión, como el certificado del servidor, la cadena de certificados, y las suites de cifrado utilizadas. Una vez establecida la conexión, es posible interactuar con el servicio de forma segura, enviando y recibiendo datos a través

de esta conexión, en este caso nuestro dato importante es la contraseña para el siguiente nivel.

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
  i:CN = SnakeOil
  a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
  v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
-----
read R BLOCK
8xCjnmgoKbGLhHFAZ1GE5Tmu4M2tKJQo
Correct!
kSkvUpMQ71BYyCM4GBPvCvT1BfWRy0Dx

closed
bandit15@bandit:~$
```

Nivel 16 = kSkvUpMQ71BYyCM4GBPvCvT1BfWRy0Dx

- ☐ Para el nivel 16 tiene varios puntos a tener en cuenta, primero debemos escanear el rango de puertos para realizar una búsqueda de cuáles están activos con nmap.
- ☐ Como hay 5 puertos habilitados, entonces verificamos cuales están en funcionamiento y cuáles no.
- ☐ En este caso, sabemos que el 31518 y 31790 están utilizando SSL, así que nos vamos con el puerto 31790 e implementamos un comando parecido del punto 14, donde tiene echo “contraseña” | openssl s_client -connect localhost: 31790 -ign_eof, con el fin de permitir enviar una cadena de texto a un servidor a través de una conexión SSL/TLS segura, manteniendo la conexión abierta para una mayor interacción con el servicio. Esto es útil para probar conexiones seguras, enviar datos sensibles, y recibir respuestas del servidor sin cerrar la conexión inmediatamente.
- ☐ Esto nos da un certificado de servidor, lo copiamos y creamos un directorio donde contenga un archivo para guardar la información, damos permisos al archivo de lectura y escritura y al crear la conexión con el ssh, ya estaremos en bandit17.
- ☐ Y podremos obtener la contraseña en /etc/bandit_pass/bandit17

```
PS C:\Users\laura> ssh bandit16@bandit.labs.overthewire.org -p 2220
```

EXERCISE

This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

```
bandit16@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit16@bandit.labs.overthewire.org's password:
```



Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on discord or IRC.

```
bandit1@bandit:~$ nmap -p 31000-32000 -sV localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 02:39 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00017s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
31046/tcp  open  echo
31518/tcp  open  ssl/echo
31691/tcp  open  echo
31790/tcp  open  ssl/unknown
31969/tcp  open  echo
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
SF-Port31790-TCP:V=7.94SVN%SSLI=7%TD=8/26%Time=66CBEAFF%P=x86_64-pc-linux
SF-xgn%GenericLines,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x2
SF:0current\x20password.\n")%r(GetRequest,32,"Wrong!\x20Please\x20enter\x
SF:20the\x20correct\x20current\x20password.\n")%r(HTTPOptions,32,"Wrong!\
SF:x20Please\x20enter\x20the\x20correct\x20current\x20password.\n")%r(RTS
SF:PRRequest,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20
SF:password.\n")%r(Help,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x
SF:20current\x20password.\n")%r(FourOhFourRequest,32,"Wrong!\x20Please\x2
SF:0Please\x20the\x20correct\x20current\x20password.\n")%r(LPDString,32,"W
SF:rong!\x20Please\x20enter\x20the\x20correct\x20current\x20password.\n")
SF:%r(SIPOptions,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20curren
SF:t\x20password.\n");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 133.23 seconds
```

```
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16 | nc localhost 31046
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
^C
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16 | nc localhost 31518
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16 | nc localhost 31691
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
^C
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16 | nc localhost 31790
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16 | nc localhost 31960
kSkvUpM07lBYyCM4GBPvCvT1BfWRv0Dx
```

```
bandit16@bandit:~$ echo kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx | openssl s_client -connect localhost:31790 -ign_eof
CONNECTED(00000000)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
  i:CN = SnakeOil
  a:PKKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
  v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIFBzCCAU+gAwIBAgIU25ha2VPaWwwHhcNMjQwNjEwMDM1OTUwWWhcNMzQwNjA4
MDM1OTUwWjATHREwDwYDVQDDAhtbmFrZU9pbDCCAiIwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwwIU25ha2VPaWwwHhcNMjQwNjEwMDM1OTUwWWhcNMzQwNjA4
MDM1OTUwWjATHREwDwYDVQDDAhtbmFrZU9pbDCCAiIwDQYJKoZIhvcNAQEL
ggIPADCCAgcCgIBANI+P5QXm9Bj21FIPsQqbqZRB5XmSZZJYaam7EIJ16Fxedf+
jXAv4d/FVqiEM4BuSNsNMMeBMx2Gq0LAFN33h+RMTjRoMb8yBsZsC063MLfXCk4p+
09gtGP7BS6Iy5XdmfY/fPHvA3JDEScdLDDmd6Lsbwhv93Q8M6POV09sv4HuS4t/
jEjr+NhE+Bjr/wDbyg7GL71BP1WPZpQnRE40zoSrt5+bZVLvODWUfwinB0fLaGRk
GmI0r5EU0Ud7HpYyoIQbiNLePGfPpHRKnmXTTEZEoxeWWAaM1VhPGqfrB/Pnca+
vAJK7i80b3kHinnmFVOScsG/YAUR94wSELeY+ULEWJaELVUntrJ5HeRDiTChivQ++
wnnjNbpalW6shopybUF3XXfhIb4NvwLWpvoKFXVtcVjL0ujF0snVvpE+MRT0wacy
tHtjZs7AS6Iy5XdmfY/fPHvA3JDEScdLDDmd6Lsbwhv93Q8M6POV09sv4HuS4t/
jEjr+NhE+Bjr/wDbyg7GL71BP1WPZpQnRE40zoSrt5+bZVLvODWUfwinB0fLaGRk
18cY64ZaF6oU8bjGK7BArDx56bRc3WFYyUBIGWAFHEuB948BcshXY7baf5jjzPmgz
mq1zdRtchQB31MOM2ii6vuTkheAvKfFf+LLH4M9SnES4NSF2hj9NnHga9V08wfhYc
x0W6qu+S8HudVF+V23yTvUNgz4Q+UoGs4sHSDesIBFqNvInnpUmtNgcR2L5PAgMB
AAGjUzBRMB0GA1UdDgQWBBTp08kfze4P9EgXNuyk7+xDGFtAYzAfBgNVHSMEGDAW
gBTp08kfze4P9EgXNuyk7+xDGFtAYzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3
DQEBcwUAAICAQAKHomtmcGqyiLnhziLe97Mq2+SuL5QgYVwfx/KYOXxv2T8ZmcR
Ae9XFhZT4jsA0UDK10Xx9aZgDGJHJLNEVTe9zWv1ONFfNxEBxQgP7hhmDBWdtj6d
taqEW/Jp06X+088tnYK9NZsvDg2YRcvOHConEMjwvEL7tQK0m+GVyQfLYg6jnrhx
egH+abucTKxabFcWSE+Vk0uJYMQcbXvB4WNKz9vj4V5Hn7/DN4xIJfko+nREw60a
-----
```

-----BEGIN RSA PRIVATE KEY-----

```
MIIEoglBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMIOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LDCDCNd2IUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUde6SFthOar69jp5RILwD1NhPx3iBI
J9nOM8OJOVToum43UOS8Yx8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxAAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtf4uNtJom+asvlpms8A
vLY9r60wYSvmZhNqBUrj7lyCtXmLu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dElkza8ky5molwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsgghifKLxrlgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/Fwjulhttx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enClvGCSx+X3l5SiWg0A
R57hJglezliVjv3aGwHwvLzvtzK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5HDI
TtieK7xRVxUI+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMly9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwGxinB3OhYimtiG2Cg5JCqIZFHxD6MjEgOiu
L8ktHMPvodBwNsSBULpG0QKBgBApITfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAglHxhdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YODjHdSOoKvDQNWu6ucyLRAWFuLSeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyRqaM
77pBAoGAMmjmlJdjp+Ez8duyn3ieo36yrttF5NSsJLABxPpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBI1O4f7HVM6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPxX8MBTakzh3
```




```
vBgysi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

```
bandit16@bandit:~$ mkdir /tmp/fcch-16
bandit16@bandit:~$ cd /tmp/fcch-16
```

```
bandit16@bandit:~$ mkdir /tmp/bandit17
mkdir: cannot create directory '/tmp/bandit17': File exists
bandit16@bandit:~$ cd /tmp/bandit17
bandit16@bandit:/tmp/bandit17$ vim sshkey.private
bandit16@bandit:/tmp/bandit17$ chmod 600 sshkey.private
bandit16@bandit:/tmp/bandit17$ vim sshkey.private
27L, 1675B written
```

```
bandit16@bandit: /tmp/ban... x + v
-----BEGIN RSA PRIVATE KEY-----
MIIIEogIBAAKCAQEAvm0kuiFmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SudyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LDCdND2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpwTMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABaoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE1laFYQwik7xfW+24pRNUdE6SFth0ar69jp5RLlWd1NhPx3iBl
J9nOM80J0VToum43U0S8YxF8WwhXriYGnc1sskbwpX0UDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9q0kwFTEQpjtF4uNtJom+asvlpms8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL5ls0mama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/FwjuLhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3L5SiWg0A
R57hJglezIiVjv3aGwHwvLZvtszK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5Hdi
TtieK7xRVxUL+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFmLy9FL2m9oQWcg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBApLTfC1H0nWiMGOU3KPwYwT006CdTkmJ0mL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHdS0oKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyZrqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrTtF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9G0tt9JP5X8MBTakzh3
vBgysi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```


```
bandit16@bandit:/tmp/bandit17$ ssh -i sshkey.private bandit17@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit16/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit16/.ssh/known_hosts).
```



```

      This is an OverTheWire game server.
  More information on http://www.overthewire.org/wargames

!!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!!! Connecting from localhost is blocked to conserve resources.
!!! Please log out and log in again.
```



Nivel 17 = EReVavePLFHtFIFsJn3hyzMlvSuSAcRD

Para este nivel utilizamos el comando `diff passwords.old passwords.new`, el cual se utiliza para comparar dos archivos de texto, en este caso `passwords.old` y `passwords.new`, y mostrar las diferencias entre ellos. `diff` es una herramienta de línea de comandos que examina los archivos línea por línea y destaca las modificaciones entre versiones. Esto resulta útil para ver cómo ha cambiado el contenido entre dos versiones de un archivo, ya sea código fuente, configuraciones, o listas. En este contexto, `passwords.old` contiene la versión anterior de los datos de contraseñas, mientras que `passwords.new` tiene la versión más reciente.

```
bandit17@bandit:~$ cat /etc/bandit_pass/bandit17
EReVavePLFHtFIFsJn3hyzMlvSuSAcRD
```

```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< bSrACvJvvBSxEM2SGsV5sn09vc3xgqyp
---
> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGLO
```

La contraseña es la nueva o la última para el siguiente nivel

Nivel 18 = x2gLTTjFwMOhQ8oWNbMN362QKxfRqGIO

Tener en cuenta que para el comando es importante agregarle el `/bin/bash` al final de entrar al nivel, o se saldrá de la conexión automáticamente.

De resto, solo es utilizar los comandos que ya conocemos y con ello leer el readme, para que nos de la contraseña.

```
PS C:\Users\laura> ssh bandit18@bandit.labs.overthewire.org -p 2220 "/bin/bash"
```

```
      _-_-_-_-_-_-_-_-_-_-_  _-_-_-_-_-  
    |   |   |   |   |   |   |   |   |   |  
    |   |   |   |   |   |   |   |   |   |  
    |   |   |   |   |   |   |   |   |   |  
    |   |   |   |   |   |   |   |   |   |  
    |   |   |   |   |   |   |   |   |   |
```

```
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames
```

```
bandit18@bandit.labs.overthewire.org's password:  
ls  
readme  
ls -ls  
total 4  
4 -rw-r----- 1 bandit19 bandit18 33 Jul 17 15:57 readme  
cat readme  
cGwPmaKXVwDUNgPAVJbWYuGHVn9zl3j8
```

Nivel 19 = cGWpMaKXVwDUNgPAVJbWYuGHVn9zI3j8

Primero debemos listar los archivos y directorios, mostrando así la información adicional; incluso los archivos ocultos. Luego, con el comando `id` mostramos la información del usuario actual y los grupos del cual pertenece el usuario. Así como ya tenemos nuestro archivo `bandit20-do` subrayado con anterioridad, se ejecuta este archivo en el directorio actual y pasará el `id` como argumento a ese archivo. Así podremos leer la contraseña en el directorio específico.

```
bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root    root    4096 Jul 17 15:57 .
drwxr-xr-x 70 root    root    4096 Jul 17 15:58 ..
-rwsr-x---  1 bandit20 bandit19 14880 Jul 17 15:57 bandit20-do
-rw-r--r--  1 root    root     220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root    root    3771 Mar 31 08:41 .bashrc
-rw-r--r--  1 root    root     807 Mar 31 08:41 .profile
bandit19@bandit:~$ id
uid=11019(bandit19) gid=11019(bandit19) groups=11019(bandit19)
bandit19@bandit:~$ ./bandi20-do id
-bash: ./bandi20-do: No such file or directory
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZiQVMN9Ghs7iQWsCfZvXQubYO
```

Nivel 20 = 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

El comando `ls -la` lista los archivos y directorios en el directorio actual, mostrando detalles completos, incluidos los archivos ocultos. Luego, `nc -nnvp 3030 <<< "contraseña" &` usa `nc` (netcat) para iniciar un servidor en el puerto 3030 que escucha conexiones entrantes y envía "contraseña" a cualquier cliente que se conecte; el símbolo `&` ejecuta este comando en segundo plano. La salida "Listening on 0.0.0.0 3030" confirma que el servidor está activo y escuchando conexiones en todas las interfaces de red. El comando `jobs` lista los procesos en segundo plano, como el que se ejecutó con `nc`. Finalmente, `./subconect 3030` ejecuta un archivo o script llamado `subconect` con el puerto 3030 como argumento, para conectarse al servidor que se ha establecido con `nc`. Así que se estaría configurando un servidor de red

que escucha en el puerto 3030, mientras que otro comando se prepara para interactuar con él

```
bandit20@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root    root    4096 Jul 17 15:57 .
drwxr-xr-x 70 root    root    4096 Jul 17 15:58 ..
-rw-r--r--  1 root    root     220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root    root    3771 Mar 31 08:41 .bashrc
-rw-r--r--  1 root    root     807 Mar 31 08:41 .profile
-rwsr-x---  1 bandit21 bandit20 15604 Jul 17 15:57 suconnect
[1]+  Done                  nc -lnvp 3030 <<< 0qXahG8Zj0VMN9Ghs7i0WsCfZyX0
UbYO
bandit20@bandit:~$ nc -lnvp 3030 <<< 0qXahG8Zj0VMN9Ghs7i0WsCfZyX0UbYO &
[1] 756186
bandit20@bandit:~$ Listening on 0.0.0.0 3030
^C
bandit20@bandit:~$ jobs
[1]+  Running              nc -lnvp 3030 <<< 0qXahG8Zj0VMN9Ghs7i0WsCfZyX0
UbYO &
```

```
bandit20@bandit:~$ ./suconnect 3030
Connection received on 127.0.0.1 33232
Read: 0qXahG8Zj0VMN9Ghs7i0WsCfZyX0UbYO
Password matches, sending next password
EeoULMCra2q0dSkYj561DX7s1CpBuOBt
```

Nivel 21 = EeoULMCra2q0dSkYj561DX7s1CpBuOBt

Primero, man cron y man 5 crontab proporcionan información sobre el funcionamiento de cron y el formato de los archivos crontab, respectivamente. Luego, ls -la /etc/cron.d lista los archivos en el directorio donde se almacenan las configuraciones de cron, permitiendo ver qué tareas están programadas. Con cat /etc/cron.d/cronjob_bandit22, se examina el contenido de un archivo de configuración de cron específico para entender qué tarea se ejecuta. Posteriormente, cat /usr/bin/cronjob_bandit22.sh muestra el script asociado a esa tarea programada para revelar qué acciones realiza. Finalmente, cat /tmp/"dato dado anteriormente" revisa el contenido de un archivo temporal, cuyo nombre se refiere a información previamente obtenida. En conjunto, estos comandos ayudan a entender y verificar la configuración y ejecución de tareas automáticas en el sistema, para así poder obtener la contraseña del siguiente nivel

```
bandit21@bandit:~$ man cron
bandit21@bandit:~$ bandit21@bandit:~$ man 5 crontab
No manual entry for crontab in section 5
bandit21@bandit:~$ man 5 crontab
bandit21@bandit:~$ bandit21@bandit:~$ ls -la /etc/cron.d
total 44
drwxr-xr-x  2 root root  4096 Jul 17 15:59 .
drwxr-xr-x 121 root root 12288 Aug  1 14:49 ..
-rw-r--r--  1 root root   120 Jul 17 15:57 cronjob_bandit22
-rw-r--r--  1 root root   122 Jul 17 15:57 cronjob_bandit23
-rw-r--r--  1 root root   120 Jul 17 15:57 cronjob_bandit24
-rw-r--r--  1 root root   201 Apr  8 14:38 e2scrub_all
-rwx-----  1 root root    52 Jul 17 15:59 otw-tmp-dir
-rw-r--r--  1 root root   102 Mar 31 00:06 .placeholder
-rw-r--r--  1 root root   396 Jan  9 2024 sysstat
```

```
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:~$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q
```

Nivel 22 = tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q

Se debe identificar un trabajo cron que se ejecuta automáticamente en el sistema.

Comienza listando y accediendo al directorio /etc/cron.d/, donde están configurados los trabajos cron. Luego, se inspecciona el archivo cronjob_bandit que define un trabajo cron específico, el cual ejecuta un script ubicado en /usr/bin/cronjob_bandit23.sh. Al revisar el contenido de este script, puedes observar que genera un hash MD5 basado en una cadena específica. Este hash es la clave, el cual está contenido en /tmp/.

```
bandit22@bandit:~$ ls
bandit22@bandit:~$ cd /etc/cron.d/
bandit22@bandit:/etc/cron.d$ ls
cronjob_bandit22  cronjob_bandit23  cronjob_bandit24  e2scrub_all  otw-tmp-dir  sysstat
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:/etc/cron.d$ /usr/bin/cronjob_bandit23.sh
Copying passwordfile /etc/bandit_pass/bandit22 to /tmp/8169b67bd894ddb4412f91573b38db3
bandit22@bandit:/etc/cron.d$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
0Zf11ioIjMVN551jX3CmStKLYqjk54Ga
bandit22@bandit:/etc/cron.d$
```

Nivel 23 = 0Zf11ioljMVN551jX3CmStKLYqjk54Ga

Para pasar este nivel nos dirigimos al mismo directorio de donde sacamos las contraseñas anteriores y notamos que el sh está apuntando al usuario de bandit 24 por lo que creamos un script en la carpeta temporal y un archivo para guardar la clave.

El script en cuestión es bastante simple solo es un apuntador que guarda la clave de bandit24 en el archivo que creamos en el directorio temporal de bandit23

```
bandit23@bandit:~$ cd /etc/cron.d/
bandit23@bandit:/etc/cron.d$ ls
cronjob_bandit22  cronjob_bandit23  cronjob_bandit24  e2scrub_all  otw-tmp-dir  sysstat
bandit23@bandit:/etc/cron.d$ cat cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
bandit23@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash

myname=$(whoami)

cd /var/spool/$myname/foo
echo "Executing and deleting all scripts in /var/spool/$myname/foo:"
for i in * .*;
do
    if [ "$i" != "." -a "$i" != ".." ];
    then
        echo "Handling $i"
        owner="$(stat --format "%U" ./.$i)"
        if [ "${owner}" = "bandit23" ]; then
            timeout -s 9 60 ./.$i
        fi
        rm -f ./.$i
    fi
done

bandit23@bandit:/etc/cron.d$ cat /var/spool/$myname/foo
cat: /var/spool//foo: No such file or directory
bandit23@bandit:/etc/cron.d$ cat /var/spool/bandit24/foo
cat: /var/spool/bandit24/foo: Permission denied
bandit23@bandit:/etc/cron.d$ cd /var/spool/bandit24/foo
bandit23@bandit:/var/spool/bandit24/foo$ ls
ls: cannot open directory '.': Permission denied
bandit23@bandit:/var/spool/bandit24/foo$ mkdir /tmp/bandit24clave
bandit23@bandit:/var/spool/bandit24/foo$ cd /tmp/bandit24clave
bandit23@bandit:/tmp/bandit24clave$ nano script.sh
Unable to create directory /home/bandit23/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.
```

```

bandit23@bandit:/tmp/bandit24clave$ ls
script.sh
bandit23@bandit:/tmp/bandit24clave$ nano script.sh
Unable to create directory /home/bandit23/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit23@bandit:/tmp/bandit24clave$ ls -l
total 4
-rw-rw-r-- 1 bandit23 bandit23 71 Aug 26 01:37 script.sh
bandit23@bandit:/tmp/bandit24clave$ cat script.sh
#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/bandit24clave/clave
bandit23@bandit:/tmp/bandit24clave$ touch clave
bandit23@bandit:/tmp/bandit24clave$ ls
clave script.sh
bandit23@bandit:/tmp/bandit24clave$ chmod 777 -R /tmp/bandit24clave
bandit23@bandit:/tmp/bandit24clave$ ls -l
total 4
-rwxrwxrwx 1 bandit23 bandit23 0 Aug 26 01:39 clave
-rwxrwxrwx 1 bandit23 bandit23 71 Aug 26 01:37 script.sh
bandit23@bandit:/tmp/bandit24clave$ cat clave
bandit23@bandit:/tmp/bandit24clave$ cat clave
bandit23@bandit:/tmp/bandit24clave$ cp script-sh /var/spool/bandit24/foo
cp: cannot stat 'script-sh': No such file or directory
bandit23@bandit:/tmp/bandit24clave$ ls
clave script.sh
bandit23@bandit:/tmp/bandit24clave$ cp script.sh /var/spool/bandit24/foo
bandit23@bandit:/tmp/bandit24clave$ cat clave
bandit23@bandit:/tmp/bandit24clave$ cat clave
bandit23@bandit:/tmp/bandit24clave$ cat clave
bandit23@bandit:/tmp/bandit24clave$ cat clave
gb8KRRcSshuZXI0tUuR6ypOFjiZbf3G8
bandit23@bandit:/tmp/bandit24clave$

```

Nivel 24 = gb8KRRcSshuZXI0tUuR6ypOFjiZbf3G8

Para este nivel es necesario crear un archivo en /bin/bash, donde debemos colocar la contraseña con la que ingresamos a este nivel y así poder iterar sobre todos los rangos que van de 0000 a 9999 y así poder enviar el PIN y la contraseña, de esta forma podremos obtener la contraseña del siguiente nivel

```

GNU nano 7.2
#!/bin/bash

bandit24-gb8KRRcSshuZXI0tUuR6ypOFjiZbf3G8

for pin in {0000..9999}; do
    echo "$bandit24 $pin | nc localhost 30002
done

```

```

Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
Correct!
The password of user bandit25 is iCi86ttT4KSNe1armKiwbQNmB3YJP3q4

bandit24@bandit:/tmp/clave24$

```

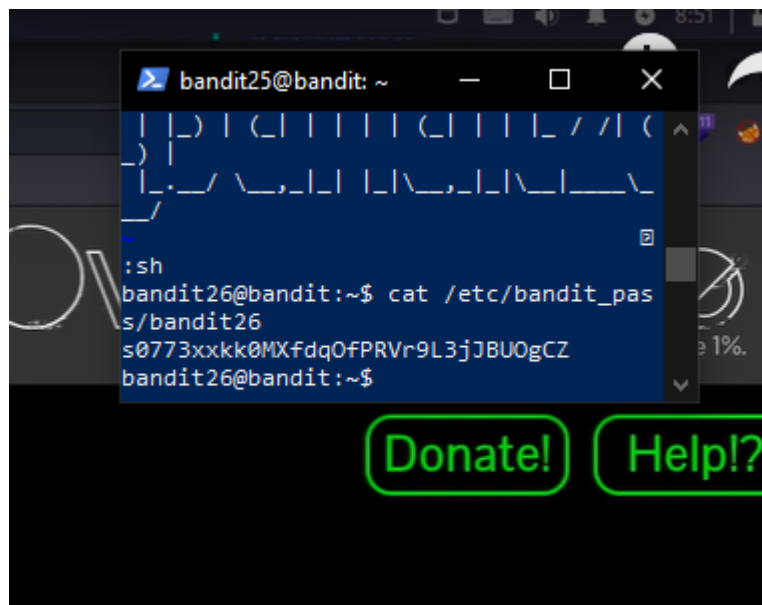
Nivel 25 = iCi86ttT4KSNe1armKiwBQNmB3YJP3q4

Para este caso solo realizaremos la conexión a SSH al servidor que se ejecuta en localhost, autenticandose como el usuario bandit26 utilizando una clave privada almacenada en el archivo bandit26.sshkey; donde la conexión se realiza a través del puerto 2220; luego solo es leer el archivo para la contraseña de bandit26 y ajustar el tamaño de pantalla para poder establecer la contraseña del siguiente nivel.

```
bandit25@bandit:~$ ssh -oHostkeyAlgorithms=+ssh-dss -i bandit26.sshkey bandit26@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLFXC5CX1hmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit25/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit25/.ssh/known_hosts).
```

bandit

This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>



Nivel 26 = s0773xxkk0MXfdqOfPRVr9L3jJBUOgCZ

para este nivel seguimos aprovechando el “bug” de more que nos permite ejecutar comandos en vi y por medio del directorio de pass obtenemos la clave de bandit 27

[illegible]

Nivel 27 = upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB

La idea de este nivel es poder clonar el repositorio desde una referencia establecida que nos dan en el enunciado del nivel, luego navegar sobre este y buscar el archivo readme, ya que por lo general en un repositorio la idea del readme es mostrar información adicional, para este caso es la contraseña del siguiente nivel.

```
bandit27@bandit:~$ mkdir /tmp/clave27
bandit27@bandit:~$ cd /tmp/clave27
bandit27@bandit:/tmp/clave27$ git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihhV1wUXRb4RrEcLFXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).

  [L] [O] [G] [I] [T]
  [D] [I] [G] [I] [T]
  [L] [O] [G] [I] [T]

      This is an OverTheWire game server.
  More information on http://www.overthewire.org/wargames

bandit27-git@localhost's password:
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), 287 bytes | 287.00 KiB/s, done.
bandit27@bandit:/tmp/clave27$ ls
repo
bandit27@bandit:/tmp/clave27$ cd repo
bandit27@bandit:/tmp/clave27/repo$ cat README
The password to the next level is: Yz9IpL0sBcCeuG7m9uQfT8ZnpS4HZRcN
bandit27@bandit:/tmp/clave27/repo$
```

Nivel 28 = Yz9lpL0sBcCeuG7m9uQFt8ZNpS4HZRcN

Para este nivel tenemos que encontrar la clave en un repositorio de git por lo que primero hacemos una carpeta en /tmp para clonar el repo y miramos el archivo que hay dentro, como ese archivo no nos proporciona la clave usamos git log para ver los commits anteriores a ese y nos cambiamos a la rama que hizo el ultimo commit, por ultimo abrimos el archivo readme y ahí encontramos las credenciales para el siguiente nivel.

Nivel 29 = 4pT1t5DENaYuqnqvadYs1oE4QLCdjmJ7

Para este nivel hacemos los mismos pasos del punto anterior hasta que llegamos al readme.txt que nos dice “no password in production” después de eso verificamos las ramas y nos cambiamos a la rama dev donde podemos encontrar la clave para este nivel..

```
bandit29@bandit:~$ mkdir /tmp/clave29
bandit29@bandit:~$ cd /tmp/clave29
bandit29@bandit:/tmp/clave29$ git clone ssh://bandit29-git@localhost:2220/home/bandit29-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEclFxC5CX1hmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit29/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit29/.ssh/known_hosts).
```

The logo for OverTheWire Wargames, featuring the words "OverTheWire" in a stylized, blocky font with a grid-like pattern, and "WARGAMES" below it in a similar style.

This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

```
bandit29-git@localhost's password:
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 16 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (16/16), 1.43 KiB | 489.00 KiB/s, done.
Resolving deltas: 100% (2/2), done.
```

```
bandit29@bandit:/tmp/clave29$ ls
repo
bandit29@bandit:/tmp/clave29$ cd repo/
bandit29@bandit:/tmp/clave29/repo$ ls
README.md
bandit29@bandit:/tmp/clave29/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: <no passwords in production!>
```



```

bandit29@bandit:/tmp/clave29/repo$ git log
commit efa5bd803f8335e5e9da5c4c7c876aefc9f8b4 (HEAD -> master, origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date:   Wed Jul 17 15:57:31 2024 +0000

    fix username

commit 5a53eb83a43bac1f0b4e223e469b40ef68a4b6e6
Author: Ben Dover <noone@overthewire.org>
Date:   Wed Jul 17 15:57:31 2024 +0000

    initial commit of README.md
bandit29@bandit:/tmp/clave29/repo$ git checkout 5a53eb83a43bac1f0b4e223e469b40ef68a4b6e6
Note: switching to '5a53eb83a43bac1f0b4e223e469b40ef68a4b6e6'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

    git switch -c <new-branch-name>

Or undo this operation with:

    git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at 5a53eb8 initial commit of README.md
bandit29@bandit:/tmp/clave29/repo$ ls
README.md
bandit29@bandit:/tmp/clave29/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit29
- password: <no passwords in production!>

```

```

bandit29@bandit:/tmp/clave29/repo$ git branch -a
* (HEAD detached at 5a53eb8)
  master
  remotes/origin/HEAD -> origin/master
  remotes/origin/dev
  remotes/origin/master
  remotes/origin/splotts-dev
bandit29@bandit:/tmp/clave29/repo$ git checkout remotes/origin/dev
Previous HEAD position was 5a53eb8 initial commit of README.md
HEAD is now at eef5340 add data needed for development
bandit29@bandit:/tmp/clave29/repo$ ls
code  README.md
bandit29@bandit:/tmp/clave29/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

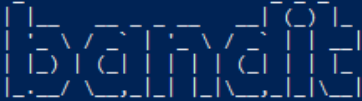
- username: bandit30
- password: qp30ex3VLz5MDG1n91YowTv4Q817CDZL

bandit29@bandit:/tmp/clave29/repo$

```

Para este nivel y como en los anteriores clonamos el repo de git y intentamos buscar la clave en el archivo readme que nos ofrece, pero en este caso nos dice que está vacío lo cual es un poco sospechoso.

```
bandit30@bandit:/tmp/clave20$ mkdir /tmp/clave30
bandit30@bandit:/tmp/clave20$ cd /tmp/clave30
bandit30@bandit:/tmp/clave30$ git clone ssh://bandit30-git@localhost:2220/home/bandit30-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnVlwUXRb4RrEcLfXCSCXlhmAAM/ureryLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit30/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit30/.ssh/known_hosts).
```



```

      This is an OverTheWire game server.
    More information on http://www.overthewire.org/wargames

bandit30-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), 297 bytes | 297.00 KiB/s, done.
bandit30@bandit:/tmp/clave30$ ls
repo
bandit30@bandit:/tmp/clave30$ cd repo/
bandit30@bandit:/tmp/clave30/repo$ la
.git README.md
bandit30@bandit:/tmp/clave30/repo$ cat README.md
just an empty file... muahaha
bandit30@bandit:/tmp/clave30/repo$ git log
commit 60410f42e05023128098dc1f6991c75e6ae02e47 (HEAD -> master, origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date:   Wed Jul 17 15:57:34 2024 +0000

    initial commit of README.md
bandit30@bandit:/tmp/clave30/repo$ git branch -a
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/master
bandit30@bandit:/tmp/clave30/repo$ git tag
secret
bandit30@bandit:/tmp/clave30/repo$ git how secret
git: 'how' is not a git command. See 'git --help'.

The most similar command is
show
bandit30@bandit:/tmp/clave30/repo$ git show secret
fb552xb7bRyFmAvQYQGEGsbhVyJqhnDy
```

Para este nivel se nos pide modificar el archivo key.txt y ponerle un texto específico “May I in you” y realizar los pasos respectivos para hacer un push, los cuales listare a continuación git add .

```
git push -u origin
```

y de esta forma podemos obtener la clave para este nivel, cabe resaltar que para este nivel como en los anteriores se clonó el repositorio y se creo un directorio en /tmp.

```
bandit31@bandit:/tmp/.cache31/repo$ nano key.txt
Unable to create directory /home/bandit31/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.
```

```
bandit31@bandit:/tmp/clave31/repo$ ll
Command 'lls' not found, did you mean:
  command 'rls' from snap rustup (1.27.1)
  command 'ils' from deb sleuthkit (4.12.1+dfsg-1)
  command 'als' from deb atool (0.39.0-13)
  command 'jls' from deb sleuthkit (4.12.1+dfsg-1)
  command 'rls' from deb rustup (1.26.0-3)
  command 'bls' from deb bacula-sd (9.6.7-7)
  command 'hls' from deb hfsutils (3.2.6-15build2)
  command 'ols' from deb speech-tools (1:2.5.0-13)
  command 'fls' from deb sleuthkit (4.12.1+dfsg-1)
  command 'ls' from deb coreutils (9.4-2ubuntu2)
See 'snap info <snapname>' for additional versions.
bandit31@bandit:/tmp/clave31/repo$ ls
key.txt  README.md
bandit31@bandit:/tmp/clave31/repo$ git add -f key.txt
bandit31@bandit:/tmp/clave31/repo$ git commit -m "Upload Key.txt"
[master e92381a] Upload Key.txt
 1 file changed, 1 insertion(+), 1 deletion(-)
bandit31@bandit:/tmp/clave31/repo$ git push -u origin master
```

```
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.  
ED25519 key fingerprint is SHA256:C2ihUBV7innVwUXRb4RrEclFXC5X1hmAAM/uerLY.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Could not create directory '/home/bandit31/.ssh' (Permission denied).  
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
```

Boydell

```

      This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

```

```
bandit31-git@localhost's password:
Enumerating objects: 10, done.
Counting objects: 100% (10/10), done.
Delta compression using up to 2 threads
Compressing objects: 100% (6/6), done.
Writing objects: 100% (9/9), 759 bytes | 759.00 KiB/s, done.
Total 9 (delta 2), reused 0 (delta 0), pack-reused 0
remote: ### Attempting to validate files... ###
remote:
remote: .o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.
remote:
remote: Well done! Here is the password for the next level:
remote: 309RfhqyAlVBEzpVb6L5tshZoqo5x5K
remote:
remote: .o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.
remote:
remote: .o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.
remote:
remote: Wrong!
remote:
remote: .o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.
remote:
To ssh://localhost:2220/home/bandit31-git/repo
+-- new file: remote: master -> master (new receive hook declined)
```

Nivel 32 = 3O9RfhqyAlVBEZpVb6LYStshZoqoSx5K

Para el último nivel solo tuvimos que buscar en `/etc/bandit_pass/bandit33` que es donde se encuentran las claves para los niveles de bandit.

```

WELCOME TO THE UPPERCASE SHELL
>> $0

$ $ $ ^[[A^[[A^C
$
$

$ $
$ 0
sh: 7: 0: Permission denied
$ pwd
/home/bandit32
$ id
uid=11033(bandit33) gid=11032(bandit32) groups=11032(bandit32)
$ cat /etc/bandit_pass/bandit33
tQdtbs5D5i2vJwkO8mEyYeyTL8izoeJ0
$

```

Nivel 33 = tQdtbs5D5i2vJwkO8mEyYeyTL8izoeJ0

En este nivel solo leemos lo que está en el readme y así concluimos que acabamos bandit y sus niveles

```

bandit33@bandit:~$ ls
README.txt
bandit33@bandit:~$ cat README.txt
Congratulations on solving the last level of this game!

At this moment, there are no more levels to play in this game. However, we are constantly working
on new levels and will most likely expand this game with more levels soon.
Keep an eye out for an announcement on our usual communication channels!
In the meantime, you could play some of our other wargames.

If you have an idea for an awesome new level, please let us know!
bandit33@bandit:~$

```

Nivel 34 = no hay xd